Constructions of lattices via biquadratic and triquadratic fields

L. F. Santos and G. C. Jorge

Abstract. The lattices D_4 and E_8 are known to be the densest lattices in dimensions 4 and 8, respectively. In this paper, we employ tools from algebraic number theory to prove that the D_4-lattice arises from an infinite family of totally imaginary biquadratic fields. Furthermore, we extend this construction to show that both the D_8 and E_8 can be realized via triquadratic fields derived from this family.

Mathematics Subject Classification (2010). 11H06, 11H31, 11R11, 11R16.

Keywords. Lattices, Packing Density, Number Fields.

1. Introduction

Lattices are discrete sets of points in the n-dimensional Euclidean space $\mathbb{R}^n$, which are described as all integer linear combinations of independent vectors. A sphere packing in $\mathbb{R}^n$ is a distribution of spheres of equal radius such that any two spheres either do not intersect or intersect only on their boundaries. A lattice packing is a sphere packing in which the set of centers of the spheres forms a lattice. The packing density of a sphere packing is the proportion of $\mathbb{R}^n$ covered by the union of the spheres of the packing. Usually, the problem of finding good signal constellations for a Gaussian channel is associated with the search for lattices with high packing density [2].

Given a number field $\mathbb{K}$ of degree n, one can construct lattices in $\mathbb{R}^n$ from $\mathbb{Z}$-modules contained in $\mathbb{K}$, using either the canonical or the twisted embedding [4, 5, 15]. A lattice obtained in this way is called an algebraic lattice. An interesting problem, both from a theoretical and a practical perspective, is to characterize which lattices can arise from certain number fields. In this paper, we focus on biquadratic and triquadratic fields, i.e., number fields of the forms $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ and $\mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{c})$, respectively, where a, b and c are square-free integers.

This work was partially supported by FAPESP 2023/05215-7, CAPES, PICME and CNPq 405842/2023-6.

The D_n-lattice is defined as the set of points in $\mathbb{R}^n$ with integer coordinates whose sum is even. The lattice packing associated with D_4 has been proven to be the densest lattice packing in $\mathbb{R}^4$, with density $\pi^2/16$ (see [14]). The E_8-lattice is defined as the set of points in $\mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8$ whose coordinate sum is even. In [18] it was proved that the sphere packing (not just the lattice packing) associated with E_8 achieves the highest possible density in dimension 8. This density is equal to $\pi^4/384$, which is precisely twice that of the packing associated with D_8, whose density is $\pi^4/768$.

Algebraic constructions of D_4 have been considered in some papers. The field $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$ is used in [1, 5, 7], while $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3}, i)$, $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$, and $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ appear in [11, 12, 13]. An infinite family of totally real biquadratic fields of the form $\mathbb{Q}(\sqrt{2}, \sqrt{q})$, where $q \equiv 3 \pmod 8$ is prime, yielding D_4-lattices, is presented in [10]. On the other hand, the case of D_8 is treated in [11, 12], based on the fields $\mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$ and $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$.

As for E_8, several constructions have been proposed. The fields $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$ were used in [8], while $\mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$, and $\mathbb{Q}(\zeta_{24})$ are employed in [5]. The field $\mathbb{Q}(\zeta_{20})$ is also considered in [1]. In [3], it is shown that there are infinitely many subfields $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{pq})$, with p and q distinct primes, that can generate rotated E_8-lattices. Further constructions involving $\mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ are presented in [6, 13].

In this paper, we focus on constructions of D_4, D_8 and E_8 via biquadratic and triquadratic fields. In Section 3, we show that D_4-lattices can be obtained via an infinite family of totally imaginary biquadratic fields of the form $\mathbb{Q}(\sqrt{2}, \sqrt{-q})$, where $q \equiv 3 \pmod 8$ is a product of primes congruent to either 1 or 3 modulo 8. In Section 4, we describe methods for constructing the lattices $D_4 \oplus D_4$, D_8, and E_8 via the triquadratic fields $\mathbb{Q}(\sqrt{2}, \sqrt{q}, i)$.

2. Preliminaries

This section presents some elementary results on algebraic lattices. More details can be found in [2, 15, 17]. Let $\Lambda \subset \mathbb{R}^n$ be a full-rank lattice and ρ the packing radius of Λ. The packing density of a lattice is given by

$$\Delta(\Lambda) = \frac{\text{Volume of the ball of radius } \rho}{\text{Volume of a fundamental region of } \Lambda} = \frac{\text{vol}(B[0,1])\,\rho^n}{\text{vol}(\Lambda)}.$$

Since for fixed n the volume of $B[0,1]$ is constant, the center density of a lattice is defined as

$$\delta(\Lambda) = \frac{\rho^n}{\text{vol}(\Lambda)}.$$

Let $\mathbb{K}$ be a CM-field of degree $n = 2r$, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ denote the n embeddings of $\mathbb{K}$ into $\mathbb{C}$, ordered such that $\overline{\sigma_{j+r}} = \sigma_j$ for $j = 1, \ldots, r$, where $\overline{\sigma_{j+r}}$ denotes the composition of σ_{j+r} with complex conjugation. The canonical embedding $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ is defined, for each $x \in \mathbb{K}$, by

$$\sigma_{\mathbb{K}}(x) = (\Re(\sigma_1(x)), \Im(\sigma_1(x)), \ldots, \Re(\sigma_r(x)), \Im(\sigma_r(x))),$$

where $\Re$ and $\Im$ denote the real and imaginary parts of a complex number, respectively. It can be shown that if $M \subseteq \mathbb{K}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{x_1, \ldots, x_n\}$, then $\sigma_{\mathbb{K}}(M)$ is a full-rank lattice in $\mathbb{R}^n$ with basis $\{\sigma_{\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{K}}(x_n)\}$. Additionally, a Gram matrix for $\sigma_{\mathbb{K}}(M)$ is given by

$$G = \frac{1}{2}\left[\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x_i\overline{x_j})\right]_{1\le i,j\le n}, \tag{2.1}$$

where $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}$ denotes the field trace, i.e., the sum of the n embeddings of $\mathbb{K}$.

We denote by $\mathcal{O}_{\mathbb{K}}$ the ring of integers of $\mathbb{K}$, which is the set of all algebraic integers in $\mathbb{K}$. If M is a $\mathbb{Z}$-submodule of $\mathcal{O}_{\mathbb{K}}$ of rank n, then the minimum Euclidean distance and volume of $\sigma_{\mathbb{K}}(M)$ are given, respectively, by

$$2^{-\frac{1}{2}} \min_{x\in M\setminus\{0\}} \sqrt{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x})} \quad \text{and} \quad 2^{-\frac{n}{2}}\sqrt{|\operatorname{Disc}(\mathbb{K})|}\cdot[\mathcal{O}_{\mathbb{K}} : M],$$

where $\operatorname{Disc}(\mathbb{K})$ represents the discriminant of the number field $\mathbb{K}$. Therefore, since ρ is half the minimum distance in Λ, the center density of $\sigma_{\mathbb{K}}(M)$ is given by

$$\delta(\sigma_{\mathbb{K}}(M)) = \frac{\left(\min_{\substack{x\in M\\ x\neq 0}} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x})\right)^{\frac{n}{2}}}{2^n\sqrt{|\operatorname{Disc}(\mathbb{K}}|\cdot[\mathcal{O}_K : M]}. \tag{2.2}$$

3. Construction of D_4 via $\mathbb{Q}\left(\sqrt{2}, \sqrt{-q}\right)$

Let $\mathbb{K} = \mathbb{Q}\left(\sqrt{2}, \sqrt{-q}\right)$ be a totally imaginary biquadratic field, where q is a positive square-free integer congruent to 3 modulo 8. Since $(-q) \equiv 1 \pmod 4$, the set $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is an integral basis for $\mathbb{K}$, with

$$\alpha_1 = 1, \quad \alpha_2 = \sqrt{2}, \quad \alpha_3 = \frac{1 + i\sqrt{q}}{2}, \quad \alpha_4 = \frac{\sqrt{2} + i\sqrt{2q}}{2}.$$

and

$$\operatorname{Disc}(\mathbb{K}) = 64q^2$$

(see [19]). Given $x = \sum_{i=1}^{4} x_i\alpha_i \in \mathcal{O}_{\mathbb{K}}$, where $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, we have:

$$x = x_1 + x_2\sqrt{2} + \frac{x_3}{2} + \frac{x_4\sqrt{2}}{2} + i\sqrt{q}\left(\frac{x_3 + x_4\sqrt{2}}{2}\right).$$

Thus,

$$\begin{aligned} x\overline{x} &= \left(x_1 + x_2\sqrt{2} + \frac{x_3}{2} + \frac{x_4\sqrt{2}}{2}\right)^2 + q\left(\frac{x_3 + x_4\sqrt{2}}{2}\right)^2 \\ &= x_1^2 + 2x_2^2 + \frac{x_3^2}{4} + \frac{x_4^2}{2} + x_1x_3 + 2x_2x_4 \\ &\quad + \sqrt{2}\left(2x_1x_2 + x_1x_4 + x_2x_3 + \frac{x_3x_4}{2}\right) + q\left(\frac{x_3^2 + 2x_4^2 + 2x_3x_4\sqrt{2}}{4}\right). \end{aligned}$$

We conclude that:

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = (2x_1 + x_3)^2 + 2(2x_2 + x_4)^2 + q(x_3^2 + 2x_4^2). \tag{3.1}$$

Proposition 3.1. *Let j be a integer such that:*

$$\mathcal{M}_{j,q} := \left\{ x = \sum_{i=1}^{4} x_i\alpha_i \in \mathcal{O}_{\mathbb{K}} \mid x_3 \equiv -2x_1 + j(2x_2 + x_4) \pmod{q} \right\}.$$

Then, $\mathcal{M}_{j,q}$ has rank 4 and index q.

Proof. Since $x_3 \equiv -2x_1 + j(2x_2 + x_4) \pmod{q}$, there exists $t \in \mathbb{Z}$ such that $x_3 = -2x_1 + j(2x_2 + x_4) + tq$. Therefore,

$$\begin{aligned} x &= x_1\alpha_1 + x_2\alpha_2 + (-2x_1 + j(2x_2 + x_4) + tq)\alpha_3 + x_4\alpha_4 \\ &= x_1(\alpha_1 - 2\alpha_3) + x_2(\alpha_2 + 2j\alpha_3) + t(q\alpha_3) + x_4(j\alpha_3 + \alpha_4). \end{aligned}$$

It is straightforward to check that the set $\{\alpha_1 - 2\alpha_3, \alpha_2 + 2j\alpha_3, q\alpha_3, j\alpha_3 + \alpha_4\}$ is linearly independent over $\mathbb{Z}$. Moreover:

$$[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_{j,q}] = \begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 2j & 0 \\ 0 & 0 & q & 0 \\ 0 & 0 & j & 1 \end{vmatrix} = q,$$

see [17, Ch. 1, Theorem 1.17]. □

Additionally, consider the following auxiliary proposition:

Proposition 3.2. *Let $q = p_1^{e_1} \cdots p_m^{e_m}$, where $m \geq 1$, p_j are distinct primes congruent to either 1 or 3 modulo 8 and $e_j \geq 1$ are integers, for $j = 1, \ldots, m$. Then, -2 is a quadratic residue modulo q.*

Proof. By [9, Ch. VI, Theorems 82 and 95], for all primes $p \equiv 1 \pmod{8}$ and $p \equiv 3 \pmod{8}$, we have -2 is a quadratic residue modulo p. Indeed,

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1.$$

It then follows from [17, pp. 287–289] that -2 is a quadratic residue modulo $q = p_1^{e_1} \cdots p_m^{e_m}$.

□

This allows us to establish the following result:

Proposition 3.3. *Let $q \equiv 3 \pmod{8}$ be a product of primes congruent to either 1 or 3 modulo 8, and let j be a integer such that $j^2 \equiv -2 \pmod{q}$. If x is a nonzero element of*

$$\mathcal{M}_{j,q} = \left\{ x = \sum_{i=1}^{4} x_i\alpha_i \in \mathcal{O}_{\mathbb{K}} \mid x_3 \equiv -2x_1 + j(2x_2 + x_4) \pmod{q} \right\},$$

then $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 4q$.

Proof. First, note that since $x_3 \equiv -2x_1 + j(2x_2 + x_4) \pmod{q}$,

$$(2x_1 + x_3)^2 \equiv -2(2x_2 + x_4)^2 \pmod{q}.$$

Thus, there exists an integer $k \geq 0$ such that

$$(2x_1 + x_3)^2 = -2(2x_2 + x_4)^2 + kq,$$

and then, by (3.1),

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = q(k + x_3^2 + 2x_4^2).$$

Note that if $|x_3| \geq 2$ or $|x_4| \geq 2$, the result follows immediately. We now consider the following cases:

1. If $x_3 = x_4 = 0$, it follows that
$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = qk.$$
If $k = 0$, then $4x_1^2 = -8x_2^2$, which is only possible if $x = 0$, a contradiction. If $k = 1$, then
$$q = 4x_1^2 + 8x_2^2 \equiv 0 \pmod{4},$$
which contradicts $q \equiv 3 \pmod{4}$. If $k = 2$, since $\gcd(2, q) = 1$,
$$q = 2x_1^2 + 4x_2^2 \equiv 0 \pmod{2},$$
again a contradiction. If $k = 3$, then
$$3q = 4x_1^2 + 8x_2^2 \equiv 0 \pmod{4},$$
equating an odd number to an even one, which is impossible. Therefore, $\mathrm{Tr}(x\overline{x}) \geq 4q$ in this case.
2. If $x_3 = 0$ and $x_4 = \pm 1$, then
$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = (k + 2)q.$$
If $k = 0$, then $4x_1^2 = -2(2x_2 \pm 1)^2$, which is impossible. If $k = 1$, then
$$q = 8x_2^2 \pm 8x_2 + 2 + 4x_1^2 \equiv 2 \pmod{4},$$
which contradicts $q \equiv 3 \pmod{4}$. Thus, $k \geq 2$, and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 4q$.
3. If $x_3 = \pm 1$ and $x_4 = 0$, it follows that
$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = (k + 1)q.$$
If $k = 0$, then $(2x_1 \pm 1)^2 = -8x_2^2$, a contradiction. If $k = 1$ or 2, then q or $2q \equiv 1 \pmod{4}$, again a contradiction. Therefore, $k \geq 3$, and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 4q$.
4. Finally, if $x_3 = \pm 1$ and $x_4 = \pm 1$, we obtain
$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = (k + 3)q.$$
Since $k = 0$ leads to a contradiction, we have $k \geq 1$, and thus $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 4q$.

□

Finally, we can establish the main result of this section:

Theorem 3.4. *Let $q \equiv 3 \pmod 8$ be a product of distinct primes congruent to either 1 or 3 modulo 8, and let j be a integer such that $j^2 \equiv -2 \pmod q$. Thus, $\sigma_{\mathbb{K}}(\mathcal{M}_{j,q})$ is equivalent to the D_4-lattice.*

Proof. Since $\mathbb{K}$ is a CM-field, $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_{j,q}] = q$ and $\text{Disc}(\mathbb{K}) = 64q^2$, using (2.2) and Proposition 3.3, we have:

$$\delta\left(\sigma_{\mathbb{K}}\left(\mathcal{M}_{j,q}\right)\right) = \frac{\left(\min_{\substack{x\in M\\ x\neq 0}} \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x})\right)^2}{2^4 \cdot \sqrt{\text{Disc}(\mathbb{K})} \cdot [\mathcal{O}_{\mathbb{K}} : \mathcal{M}_{j,q}]} \geq \frac{(4q)^2}{16 \cdot 8q \cdot q} = \frac{1}{8}.$$

As shown in [14], the lattice D_4 has center density $\frac{1}{8}$, which is the maximum possible among lattices in $\mathbb{R}^4$. Thus,

$$\delta\left(\sigma_{\mathbb{K}}\left(\mathcal{M}_{j,q}\right)\right) = \frac{1}{8}.$$

Moreover, since the densest 4-dimensional lattice packing is unique (see [2], p. 15), the lattices of the form $\sigma_{\mathbb{K}}(\mathcal{M}_{j,q})$ are equivalent to D_4.

□

By Dirichlet's Theorem [9, Ch. II, Theorem 15], there are infinitely many primes congruent to either 1 or 3 modulo 8. Thus, there are infinitely many integers q that satisfy the conditions of Theorem 3.4.

4. Construction of D_8 and E_8 via $\mathbb{Q}\left(\sqrt{2}, \sqrt{q}, i\right)$

In this section, consider $\mathbb{L} = \mathbb{Q}\left(\sqrt{2}, \sqrt{q}, i\right)$ a totally imaginary triquadratic field, where q has the same properties as in Theorem 3.4.

Proposition 4.1. *Let $\{z_1, z_2, z_3, z_4\}$ be a $\mathbb{Z}$-basis for $\mathcal{M}_{j,q}$ and $\mathcal{S}$ be the $\mathbb{Z}$-module generated by $\{z_1, z_2, z_3, z_4, iz_1, iz_2, iz_3, iz_4\}$. Then, $\sigma_{\mathbb{L}}(\mathcal{S})$ is equivalent to $D_4 \oplus D_4$.*

Proof. Since $z_i \in \mathbb{K} = \mathbb{Q}\left(\sqrt{2}, \sqrt{-q}\right)$ for all $1 \leq j, k \leq 4$, using trace properties:

$$\begin{aligned}
&\text{Tr}_{\mathbb{L}/\mathbb{Q}}(z_j\overline{z_k}) = 2\,\text{Tr}_{\mathbb{K}/\mathbb{Q}}(z_j\overline{z_k}),\\
&\text{Tr}_{\mathbb{L}/\mathbb{Q}}(iz_j\overline{iz_k}) = \text{Tr}_{\mathbb{L}/\mathbb{Q}}(z_j\overline{z_k}) = 2\,\text{Tr}_{\mathbb{K}/\mathbb{Q}}(z_j\overline{z_k}) \text{ and}\\
&\text{Tr}_{\mathbb{L}/\mathbb{Q}}(iz_j\overline{z_k}) = \text{Tr}_{\mathbb{L}/\mathbb{Q}}(z_j\overline{iz_k}) = 0.
\end{aligned}$$

Then, by (2.1), the Gram matrix of $\sigma_{\mathbb{L}}(\mathcal{S})$ is given by

$$G = 2\begin{bmatrix} G' & 0 \\ 0 & G' \end{bmatrix},$$

where G' is a Gram matrix of $\sigma_{\mathbb{K}}(\mathcal{M}_{j,q})$ associated with $\{z_1, z_2, z_3, z_4\}$. Thus, $\sigma_{\mathbb{L}}(\mathcal{S})$ is equivalent to $D_4 \oplus D_4$. □

Classical Gram matrices, respectively, for the lattices D_4 and $D_4 \oplus D_4$ are

$$G_1 = \begin{bmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix} \quad \text{and} \quad G_2 = \begin{bmatrix} G_1 & 0 \\ 0 & G_1 \end{bmatrix}. \tag{4.1}$$

Since $\sigma_{\mathbb{K}}(\mathcal{M}_{j,q})$ is equivalent to D_4, there exist $\gamma \in \mathbb{R} \setminus \{0\}$ and a unimodular matrix U such that $G_1 = \gamma U G' U^t$ (see [2]). Moreover, if

$$\begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} = U \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix}, \tag{4.2}$$

then G_1 and G_2 are Gram matrices derived from the $\mathbb{Z}$-bases $\{w_1, w_2, w_3, w_4\}$ of $\mathcal{M}_{j,q}$ and $\{w_1, w_2, w_3, w_4, iw_1, iw_2, iw_3, iw_4\}$ of $\mathcal{S}$, respectively, up to scale factors.

In a specific case, the following proposition provides an explicit description of U and, consequently, of $\{w_1, w_2, w_3, w_4\}$.

Proposition 4.2. *Let $q = 4k^2 + 4k + 3$, $j = 2k + 1$ and*

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ j & 1 & 0 & 0 \\ -k & -k-1 & 1 & 0 \\ -1 & k & -1 & 1 \end{bmatrix},$$

where $k \in \mathbb{Z}$. If $z_1 = \alpha_1 - 2\alpha_3$, $z_2 = \alpha_2 + 2j\alpha_3$, $z_3 = q\alpha_3$ and $z_4 = j\alpha_3 + \alpha_4$, then the Gram matrix $G_{j,q}$ associated to $B = \{z_1, z_2, z_3, z_4\}$ satisfies $G_1 = \frac{1}{q} U G_{j,q} U^t$, where G_1 is given by (4.1).

Proof. First, note that $q \equiv 3 \pmod 8$. Indeed, since $l = k(k+1)/2 \in \mathbb{Z}$, we have

$$q = 4k^2 + 4k + 3 = 4k(k+1) + 3 = 8l + 3 \equiv 3 \pmod 8.$$

Moreover, we have that

$$j^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv -2 \pmod q.$$

Next, note that, by the proof of Proposition 3.1, B is a $\mathbb{Z}$-basis of $M_{j,q}$, and, by direct computation, we obtain: $z_1 = -i\sqrt{q}$, $z_2 = j + \sqrt{2} + ji\sqrt{q}$, $z_3 = \dfrac{q + qi\sqrt{q}}{2}$ and $z_4 = \dfrac{j + \sqrt{2} + ji\sqrt{q} + i\sqrt{2q}}{2}$. Then, the Gram matrix of $\sigma_{\mathbb{K}}(\mathcal{M}_{j,q})$ associated to B is

$$G_{j,q} = q \begin{bmatrix} 2 & -2j & -q & -j \\ -2j & \frac{2j^2q + 2j^2 + 4}{q} & j(q+1) & \frac{j^2q + j^2 + 2}{q} \\ -q & j(q+1) & \frac{q(q+1)}{2} & \frac{j(q+1)}{2} \\ -j & \frac{j^2q + j^2 + 2}{q} & \frac{j(q+1)}{2} & \frac{(j^2+2)(q+1)}{2q} \end{bmatrix}.$$

Substituting the values of q and j into the matrix, we obtain $G_1 = \frac{1}{q} U G_{j,q} U^t$. □

In the following theorems, consider that G_1 from (4.1) is the Gram matrix derived from the set $\{w_1, w_2, w_3, w_4\}$ from (4.2), up to scaling.

Theorem 4.3. *Let* $v = \frac{i-1}{2}w_1 + \frac{-i-1}{2}w_2 - w_3 - w_4$. *Then the set*

$$B_1 = \{w_1, w_2, w_3, w_4, v, iw_2, iw_3, iw_4\}$$

is a basis for a $\mathbb{Z}$*-module* $\mathcal{M}$ *such that* $\sigma_{\mathbb{L}}(\mathcal{M})$ *is a lattice equivalent to* D_8.

Proof. From (2.1), we have that, for all $1 \leq j, k \leq 4$,

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_j\overline{iw_k}) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_j\overline{w_k}) = 2g_{jk}, \\ \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_j\overline{w_k}) &= 0, \end{aligned} \tag{4.3}$$

where g_{jk} are the entries of G_1 from (4.1), up to scaling. Moreover, given $u \in B_1$, it follows from the linearity properties of the trace that:

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v\overline{u}) = \frac{1}{2}\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_1\overline{u}) - \frac{1}{2}\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_1\overline{u}) - \frac{1}{2}\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_2\overline{u}) \\ - \frac{1}{2}\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_2\overline{u}) - \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_3\overline{u}) - \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_4\overline{u}). \end{aligned}$$

Thus, using (4.3), we compute:

u	w_1	w_2	w_3	w_4	v	iw_2	iw_3	iw_4
$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v\overline{u})$	0	0	0	-2	4	-2	0	0

Therefore, by (2.1), since $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(u\overline{v}) = \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v\overline{u})$, the Gram matrix, up to scaling, associated with B_1 is:

$$\begin{bmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}, \tag{4.4}$$

which is a classical Gram matrix of D_8. □

Theorem 4.4. *Let* $v_1 = w_1 - w_2, \quad v_2 = \frac{i-1}{2}w_1 + \frac{-i-1}{2}w_2 - w_3 - w_4$, *and*

$$v_3 = (i+1)w_1 + (i+1)w_3 + \frac{i+1}{2}(w_2 + w_4).$$

Then the set

$$B_2 = \{v_1, w_2, w_3, w_4, v_2, iw_2, iw_3, v_3\}$$

is a basis for a $\mathbb{Z}$*-module* $\mathcal{M}$ *such that* $\sigma_{\mathbb{L}}(\mathcal{M})$ *is a lattice equivalent to* E_8.

Proof. First, note that v_2 is the same element as v from Theorem 4.3. Therefore, we only need to compute the entries of the Gram matrix involving v_1 and v_3. For any $u \in B_2$, by the linearity properties of the trace, we have:

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v_1\overline{u}) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_1\overline{u}) - \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_2\overline{u}),\\
\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v_3\overline{u}) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_1\overline{u}) + \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_1\overline{u}) + \frac{1}{2}\,\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_2\overline{u})\\
&\quad + \frac{1}{2}\,\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_2\overline{u}) + \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_3\overline{u}) + \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_3\overline{u})\\
&\quad + \frac{1}{2}\,\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(iw_4\overline{u}) + \frac{1}{2}\,\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_4\overline{u}).
\end{aligned}$$

Thus, using (4.3), we compute:

u	v_1	w_2	w_3	w_4	v_2	iw_2	iw_3	v_3
$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v_1\overline{u})$	8	-4	0	0	0	0	0	2
$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v_3\overline{u})$	2	0	0	0	0	0	0	4

Therefore, by (2.1), since $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(u\overline{v}) = \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(v\overline{u})$, the Gram matrix, up to scaling, associated with B_2 is:

$$\begin{bmatrix}
4 & -2 & 0 & 0 & 0 & 0 & 0 & 1\\
-2 & 2 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 2 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 2 & -1 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 2 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 2 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{bmatrix}, \tag{4.5}$$

which is a classical Gram matrix of E_8. □

References

[1] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito and S. I. R. Costa, Constructions of algebraic lattices, Comput. Appl. Math. **29** (2010), 1-13.

[2] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups. 3rd Edition, Springer Verlag, New York, 1999.

[3] A. L. Flores, J. C. Interlando, T. P. da Nóbrega Neto and A. L. Contiero, A new number field construction of the lattice E_8, Beitr. Algebra Geom. **54** (2013), 503-508.

[4] E. Bayer-Fluckiger, Ideal lattices, Proceedings of the Conference Number Theory and Diophantine Geometry, Zurich, 1999, Cambridge Univ. Press (2002), 168-184.

[5] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. **241** (1999), 69-84.

[6] E. Bayer-Fluckiger and I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, Arch. Math. **86**(3) (2006), 217-225.

[7] J. Boutros, E. Viterbo, C. Rastello and J. C. Belfiori, Good lattice constellations for both Rayleigh fading and Gaussian channels, IEEE Trans. Inform. Theory **42**(2) (1996), 502-517.

[8] M. Craig, A cyclotomic construction of the Leech's lattice, Mathematika **25** (1978), 236-241.

[9] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers. Sixth edition, Oxford University Press, Oxford, 2008.

[10] J. C. Interlando, J. O. D. Lopes and T. P. da Nóbrega Neto, A new number field construction of the D_4 lattice, Int. J. Appl. Math. **31**(2) (2018), 299-305.

[11] G. C. Jorge, A. J. Ferrari and S. I. R. Costa, Rotated D_n lattices, J. Number Theory **132** (2012), 2397-2406.

[12] G. C. Jorge and S. I. R. Costa, On rotated D_n-lattices constructed via totally real number fields, Arch. Math. **100** (2013), 323-332.

[13] G. C. Jorge, A. A. de Andrade, S. I. R. Costa and J. E. Strapasson, Algebraic constructions of densest lattices, J. Algebra **429** (2015), 218-235.

[14] A. Korkine and G. Zolotareff, Sur les formes quadratique positive quaternaires, Math. Ann. **5** (1872), 581-583.

[15] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.

[16] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. **27** (1948), 379-423.

[17] I. Stewart, Algebraic Number Theory and Fermat's Last Theorem. 4th ed., Chapman and Hall/CRC, New York, 2015.

[18] M. S. Viazovska, The sphere packing problem in dimension 8, Ann. Math. **185**(3) (2017), 991-1015.

[19] K. S. Williams, Integers of biquadratic fields, Can. Math. Bull. **13**(4) (1970), 519-526.

L. F. Santos and G. C. Jorge
Institute of Science and Technology
Federal University of São Paulo (UNIFESP)
São José dos Campos - Brazil
e-mail: `leonardo.farias@unifesp.br`
e-mail: `grasiele.jorge@unifesp.br`